



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

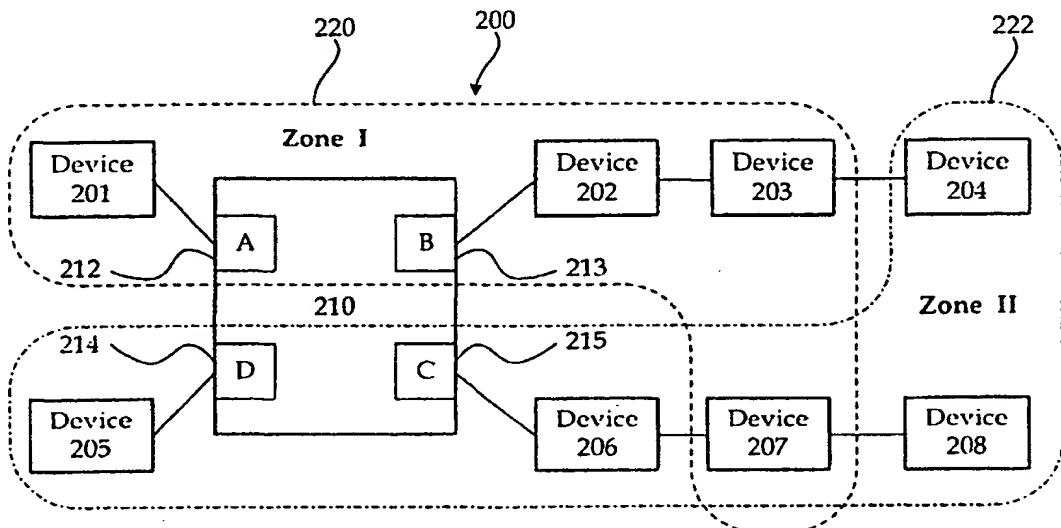
(51) International Patent Classification 7 : G06F 15/173, 13/28, 9/00		A1	(11) International Publication Number: WO 00/55750 (43) International Publication Date: 21 September 2000 (21.09.00)
(21) International Application Number: PCT/US00/06920			(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
(22) International Filing Date: 15 March 2000 (15.03.00)			
(30) Priority Data: 60/124,494 15 March 1999 (15.03.99) US 09/357,412 20 July 1999 (20.07.99) US			
(71) Applicant: SMARTSAN SYSTEMS, INC. [US/US]; 4655 Old Ironsides Drive, Suite 480, Santa Clara, CA 95054 (US).			
(72) Inventors: GAJJAR, Kumar, 1700 Fan Street, San Jose, CA 95131 (US). IBRAHIM, Mohm; 529 North 4th Street, San Jose, CA 95112 (US).			
(74) Agents: YEE, Susan et al.; Carr & Ferrell LLP, 2225 East Bayshore Road, Suite 200, Palo Alto, CA 94303 (US).			

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SYSTEM AND METHOD OF ZONING AND ACCESS CONTROL IN A COMPUTER NETWORK



(57) Abstract

A system and method for zoning devices (201–208) in a computer network (200), comprising a zone configuration database listing connected devices (201–208). The database includes for each device (201–208) an associated zone mask identifying specific zones (220, 222) of which each device (201–208) is a member. The database allows access between devices (201–208) that are members of the same zone, (220, 222) and denies access between devices (201–208) that are not members of the same zone (220, 222).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

SYSTEM AND METHOD OF ZONING AND ACCESS CONTROL IN A COMPUTER NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

5 The present application is related to, and claims priority in, co-pending U.S. Provisional Patent Application Serial No. 60/124,494, entitled "System and Method for Zoning and Access Control, Event Management, and Network Management in a Computer Network," filed on March 15, 1999.

10

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to zoning in a computer network, and more particularly to creating zones or virtual groups in a computer network such as a Storage Area Network (SAN).

2. Description of the Background Art

The introduction of fibre channel has allowed greatly increasing network connectivity between servers and storage so that many more devices can be connected to a network.

20 Fibre channel is an ANSI-standard, high-speed data communications technology providing gigabit-per-second transmission rates for storage/server and high-performance networking environments.

Increases in computer network connectivity generally require controlling access between various devices by a method such as zoning, which is a way of partitioning a large set of objects into virtual groups. In a SAN, the partitions are created between the devices connected to the SAN. The prior art for zoning computer networks allows zoning only up to the port level.

FIG. 1 shows a general prior art network configuration 100 with a plurality of devices 101-108 attached to a networking device 110, such as a router, bridge, hub, or switch. Port A 112 and port B 114 are members

of zone I 116; this indicates that all of the devices 101-104 connected to these two ports are members of zone I 116.

To be added to zone I 116, a device needs to be connected through port A 112 or port B 114. For example, to include device 107 in zone I 116, device 107 must be disconnected from port C 118 and re-connected to port A 112 or to port B 114. Similarly, to remove a device from zone I 116, the device one must be disconnected from the port that is a member of zone I 116.

Therefore, there remains a need for an improved system and method to provide a quick and easy way of zoning of devices across ports without physically moving the devices between ports.

SUMMARY OF THE INVENTION

The present invention provides a system and method for computer network zoning up to the device level, including any logical devices.

5 The invention includes a zone configuration database which is created and managed by a program running on a device connected to the computer network, and is stored in a non-volatile memory on at least one network device such as a router, a bridge, a hub, a switch, or a network master connected to the computer network. The zone configuration
10 database lists each device connected to the computer network, allows access between devices that are members of the same zone, and denies access between devices that are not members of the same zone. The zone configuration database includes a zone mask identifying zones of which each device is a member. The zone mask includes a read mask and a
15 write mask. If the read mask for a device is enabled in a particular zone then the device is granted read only access within that zone, and if the write mask for the device is enabled in the particular zone then the device is granted read and write access within that zone.

20 Other advantages and features of the present invention will be apparent from the drawings and detailed description as set forth below.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating prior art wherein zones are established at the port level;

5

FIG. 2 is a block diagram illustrating how the present invention in one embodiment can establish zones at the device level;

10 FIG. 3 is a block diagram illustrating how the invention in another embodiment can establish zones at the device level across multiple routers or network devices;

15 FIG. 4 is a block diagram illustrating how the invention in yet another embodiment can establish zones at the device level across multiple routers or network devices;

FIG. 5 is a block diagram of one embodiment of a network device according to the invention embodying a processor module for managing multiple zones in a computer network;

20

FIG. 6 is a diagram of one embodiment of the zone configuration database in the processor module of FIG. 5;

25

FIG. 7 is a block diagram of one embodiment of the device control blocks in the processor module of FIG. 5;

FIG. 8 is a diagram of one embodiment of the zone mask parameters used in the device control blocks of FIG. 7;

30

FIG. 9 is a block diagram of one embodiment of the zone control blocks in the processor module of FIG. 5;

FIG. 10 is a diagram of one embodiment of the zone mask used in the zone control blocks of FIG. 9; and

5 FIG. 11 is a flowchart of a method for initializing and establishing zones in a computer network according to the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

5 The present invention relates to an improved system and method for providing zoning in a computer network that spans all the way up to the device level, including logical devices.

FIG. 2 is a block diagram of the invention in a network configuration 200 such as a storage-area network (SAN), wherein a plurality of physical or logical devices 201-208 are connected via a network box 210, such as a router, bridge, hub, or switch, having ports 10 A-D, 212-215. The devices can be zoned at the device level regardless of port location, and also can be members of multiple zones. Device zoning is controlled through the network box 210 and is preferably configured by a program running on a master computer managing the computer network 200.

15 In FIG. 2, device 201 connected to port A 212, devices 202 and 203 connected to port B 213, and device 207 connected to port C 215 are all members of zone I 220, and device 201 is the initiating device controlling access in zone I. Device 204, even though it is connected to port B, is not a member of zone I 220. Additionally, in the chain of devices connected 20 to port C 215, the middle device 207 is the only member of zone I 220, even though device 207 connects through device 206.

FIG. 2 also shows a second zone II 222 which includes devices 204, 205, 206, 207 and 208, wherein device 205 is the initiating device controlling access in zone II. Device 207 is a member of both zone I 220 and zone II 222, and illustrates how a device can be a member of multiple zones.

It should be noted that if an initiating device is connected by a bus directly to another device then, regardless of zone membership, the two devices can communicate with each other. For example, in FIG. 2 if 30 device 204 were an initiating device, then it could communicate with devices 202 and 203.

FIG. 3 is a block diagram of another computer network configuration 300 illustrating how device level zones can be established across multiple network boxes 310 and 312. Devices 301-307 are all connected to both network boxes 310 and 312. Device 301 is connected to both A ports 314 and 322; devices 302-304 are connected to both B ports 316 and 324; device 305 is connected to both D ports 320 and 328; and devices 306 and 307 are connected to both C ports 318 and 326. The network boxes 310 and 312 control the zoning of these devices. The FIG. 3 type of configuration allows using multiple boxes with redundant paths to access devices within a zone.

The zone configuration information is stored in both network boxes 310 and 312. After one of the network boxes has been programmed with a zoning configuration, and/or after an initialization phase has been conducted by either network box, the other network box, based on already-known information as to the location of the other network box, is automatically updated.

FIG. 3 devices 301, 303 and 307 are members of zone I 320. Thus whichever network box handles a request, device 301 can access only devices 303 and 307. This feature allows users more control over access to their networked devices and allows network administrators the flexibility to configure networks without physically moving devices or changing ports.

The FIG. 4 diagram illustrates how a more sophisticated network 400 can establish zones at the device level, or more generally, between multiple network routers or boxes 420 and 422 which are configured to control zoning. A LAN/WAN 410 is connected through router 420 to a SAN 430, which in turn is connected to devices 441-443. The LAN/WAN 410 is also connected through router 422 to a SAN 432, which in turn is connected to devices 444-446. Zone I 450 is configured to include only devices 443 and 444, even though they are only connected through both SANs 430, 432, both routers 420, 422 and LAN/WAN 410.

FIG. 5 is a block diagram illustrating one embodiment of a network device or router 500 embodying a processor module 510 for managing multiple zones in a computer network. The router 500 has fibre channel input/output ports 512 and 513, as well as generic input/output ports 514, 515, 516 that can handle multiple networking protocols such as Gigabit-Ethernet (GE), ATM (Asynchronous Transfer Mode), and SCSI (Small Computer System Interface). The input/output ports 512-516 are interconnected with the processor module 510 and a cache/staging module 518.

The processor module 510 includes a processor 522, a RAM 524, a non-volatile memory 526, and a ROM 528. After initialization, the RAM 524 includes a set of device control blocks 530 and zone control blocks 532. More details of the device control blocks 530 and zone control blocks 532 are shown in, and described in conjunction with, FIGs. 7-10. The non-volatile memory 526 includes a zone configuration database 534 that stores all the information necessary to create and manage zones on a computer network (not shown) connected through the router 500.

FIG. 6 is a block diagram of one embodiment of the zone configuration database 534 in the processor module 510 of FIG. 5. The zone configuration database 534 preferably includes a structure header 610, zone information 620, fibre channel (FC) device information 630, and SCSI/other device information 640.

The structure header 610 includes standard information identifying the zone configuration database 534, including signature, checksum, version number and size.

The zone information 620 identifies each zone configured on the computer network from Zone ID 0 to Zone ID n; this identification can include an alias name for each zone, a zone ID, a zone mask number, and flags.

The FC device information 630 includes general and zone information on each connected FC device. The preferred embodiment has information for two ports, port 0 and port 1. The information for each

port generally includes a port header with identifying information such as the port number, a checksum, flags, and a device count. The port information also includes a listing of each device connected through that port. An FC port can support up to 126 devices, indicated by device 0 to device 125. Since zones can be on the level of devices, the information includes the configuration of each connected FC device; in terms of for example a WWN, flags, a read/write mask, and a read-only mask. The read/write mask and the read-only mask define the zones in which each device has read/write access, read only access, or no access.

The SCSI/other device information 640 includes general and zone information on each of the other devices, such as SCSI, ATM, or Gigabit Ethernet devices, connected to the (FIG. 5) router 500. The preferred embodiment has four ports or buses, indicated by bus 0 - bus 3. The information for each bus generally includes a bus header, bus number, checksum, flags, device count, and a listing of the devices connected through the bus. The information for each bus can also include a listing of each logical device associated, through a logical unit number (LUN), with each device. A SCSI bus can support up to 16 devices, indicated by device 0 to device 15, through each port. Each device can use logical unit numbers (LUN's) to identify up to 8 logical devices. Since zones can be specific to each physical and logical device as with the FC device information 630, SCSI/other device information 640 includes the configuration of each device connected through its corresponding bus; a unique ID, flags, a read/write mask, and a read-only mask. The read/write mask and the read-only mask define the zones in which each physical and logical device has read/write access, read-only access, or no access.

During initialization of the router 500, or if a user requests a rescan, router 500 scans all enabled ports for connected devices and creates a device control block 530 and a zone control block 532, for creating and managing zones, including: port number, port type, port ID,

device ID (SCSI ID or Fibre Channel WWN), device type, and any other information gathered by an inquiry command or other means.

Every time a zone is created, the zone configuration database 534 information is updated in the non-volatile memory 526 (FIG. 5). This 5 information includes the zone ID, zone mask information, and zone name. The network boot-up routine reads the zone configuration database 534 from the non-volatile memory 526 into the main memory 524 to set the zone mask in the device control blocks 530 and to create zone control blocks 532.

10 FIG. 7 is a block diagram of an embodiment of the device control blocks 530 in processor module 510, which are created from information received from the devices and the zone configuration database 534. Each device control block 530 corresponds to a respective physical or logical device connected to the router 500. The device control blocks 530 15 include general information required for programming purposes, such as a structure header, ID, type, state, read capacity data, inquiry data, disconnect parameters, and statistical data, and also include zone mask parameters 700 for each connected device.

20 As shown in greater detail in FIG. 8, the zone mask parameters 700 for each physical or logical device define the zone or zones of which the device is a member, and what type of access each physical or logical device is granted. The zone mask 700 preferably includes masks for up 25 to 32 different zones 802 labeled from 0 to 31. The zone mask 700 parameters include two vectors of binary numbers specifying whether the device has read only access 804, read/write access 806, or no access. Each vector is a 32 bit unsigned integer, although other length vectors 30 may be used instead. Each bit of the vector corresponds to a particular zone. If bit 0 of the vector is set to 1, then the device is a member of Zone ID 0, and so on. Thus, a 32 bit mask can support 32 zones, any number of which a device can be a member of. For example, if the device has read-only access only in zones 0 and 4, then 1s are written into the 0th and 4th positions of the read-only vector 804, and 0s are written into all

remaining positions. If the device has read/write access only in zones 1 and 3, then 1s are written into the 1st and 3rd positions of the read/write vector 806, and 0s are written into all remaining positions of the vector.

The read-only mask 804 is only used on devices that are of a read-write type, i.e. disk drive. This mask 804 allows system administrators to dynamically control read/write access of a device. Mask 804 is also useful if a device is member of multiple zones and allows only some zones to have full (read/write) access while the rest of the zones have only read access.

FIG. 9 is a block diagram of an embodiment of the processor module 510 zone control blocks 532, which are created from information stored in zone configuration database 534 and in device control blocks 530. Each zone control block 532 names all of the physical or logical devices that are members of a respective zone. The zone control blocks 532 each include general information required for programming purposes, such as a structure header, alias name, ID, flags, state, FC device count, SCSI device count, pointers to FC device control blocks, pointers to SCSI device control blocks, and a zone mask 900 identifying the particular zone managed by the zone control block.

As shown in greater detail in FIG. 10, the zone mask 900 defines the members in the zone. Zone mask 900 preferably covers up to 32 zones 1002 labeled from 0 to 31. The zone mask 900 includes a 32 bit unsigned integer (although other length numbers could be used) specifying which zone is managed by the zone block 532. Each bit of the array corresponds to a zone, but since each zone control block 532 manages only one zone, only one bit of the number is set to 1 while the remaining bits are set to 0. For whichever zone has its bit set to 1 in zone mask 900, the zone control block 532 stores the necessary information, such as pointers, to access all of the devices or logical devices identified in the zone control block 532 as members of that zone.

During operation, when a zone-managing router or network box receives an I/O request, the read-only 804 and read/write 806 zone mask

700 of the initiating device are logically ORed and the sum is logically ANDed with the read-only 804 zone mask 700 of the target node. If the product is non-zero, then both nodes belong to at least one zone in common, and if the I/O request is a read request then access is allowed,
5 otherwise the request is rejected. If the product is zero, then the read-only 804 and read/write 806 zone mask 700 of the initiating device are logically ORed and the sum is ANDed with the read/write 806 zone mask 700 of the target node. If the product is non-zero, then both nodes belong to at least one zone in common and access is allowed, otherwise
10 the request is rejected.

FIG. 11 is a flowchart of steps in a method for initializing and establishing zones in a computer network. Prior to initialization, step 1100 "discovers" all devices connected to the network and builds device control blocks (DCBs). At step 1102 the network box or router 500 (FIG. 15) 5) starts zoning initialization. At step 1104, the processor reads in the zone configuration database (ZCDB) from the non-volatile RAM into the RAM and verifies checksums. Step 1106 then begins the process of building zone control blocks (ZCBs). First, step 1108 locates a valid zone in the zone configuration database. If step 1110 determines that a valid 20 zone exists, then step 1112 allocates a zone control block and includes necessary information from the zone configuration database in the zone control block. Then the process reverts to step 1108 to build more zone control blocks. If step 1110 determines that no valid zone exists, then 25 step 1114 determines whether all the zones were checked. If not all of the zones were checked, then the process reverts to step 1108 to continue checking all of the zones. If step 1114 determines that all of the zones were checked, then the process continues to step 1116 where each device control block is analyzed.

Step 1118 begins analyzing a device control block by retrieving the 30 device ID from the (next) device control block. Then, step 1120 attempts to locate the device in the zone configuration database. If step 1122 does not find the device in the zone configuration database, then step 1124

sets the device to the default zone mask (preferably bit 31) in the device control block, adds information on the new device to the zone configuration database and the method proceeds to step 1138. If in step 1122 the device is found in the zone configuration database, then step 5 1126 fills the zone mask's (the read mask and the write mask) information from the zone configuration database into the corresponding zone information fields in the device control block. In order to fill in a list of members in the zone control block, at step 1128 the zone control block zone mask is compared with the device control block's zone mask (logical 10 OR comparison of the read mask with the write mask). At step 1130 if the zone mask of the zone control block is present in the zone masks of the device control block, then step 1132 adds a pointer of the device control block to the member list of the zone control block. Whether or not the masks match in step 1130, next, step 1134 determines whether 15 all of the zone masks of the zone control blocks have been compared with the zone mask of the device control block; and if not, then step 1136 selects the next zone control block and returns the process to step 1130, which compares the next zone mask until the zone masks of all the zone control blocks have been compared with the zone mask of the current 20 device control block.

Once all the zone control blocks have been done in step 1134, next, step 1138 determines whether all of the device control blocks have been analyzed; if not, then the process return to step 1118 for the next device control block. After step 1138 determines that all of the device control 25 blocks have been analyzed, then at step 1140 the zoning initialization is completed.

The zoning features of this invention can span multiple boxes. Zones are preferably configured using a GUI application which runs on a host PC. After every zone configuration change, the zone information is 30 sent to all the necessary routers or boxes in the same redundancy group. This feature allows users to configure networks using multiple routers with redundant paths to access their devices.

A special protocol can be implemented in the routers to allow the routers to communicate and exchange zone information with each other. At configuration time, each router is made aware of the other routers (in a redundancy group) that are connected to the same (some or all) devices in the network. Whenever there is a change in the zone database, the information will be sent to all other routers in the same redundancy group.

The software used to manage the zoning of the network preferably provides for various types of commands that allow a network administrator to create and manage the zones on the computer network. Such commands preferably include: create zone, add member to a zone, remove member from a zone, and delete zone.

Create zone is used for creating a zone in the computer network. The parameters for this command include a list of members or devices to be included in the zone. The new zone would then occupy an unused zone ID and set zone information in the zone configuration database. The corresponding zone mask is then set in the device database.

Add member to a zone is used for adding member(s) to an already existing zone. The parameters for this command include zone ID and a list of new members or devices to be added.

Remove member from a zone is used for removing member(s) from an already existing zone. The parameters include zone ID and a list of members that are to be removed.

Delete zone is used for deleting an already existing zone. The parameters for this command are the zone ID of the zone to be deleted.

The invention has been explained above with reference to a preferred embodiment. Other embodiments will be apparent to those skilled in the art in light of this disclosure. For example, the invention may be implemented in other configurations and/or used with other systems. Therefore, these and other variations upon the preferred embodiments are intended to be covered by the appended claims.

What is claimed is:

1. A method of zoning devices in a computer network, comprising the steps of:
 - 5 providing a zone configuration database identifying zones of which each device is a member; and
 - allowing zone access between devices if and only if they are members of the same zone.
- 10 2. The method of claim 1 wherein said zone configuration database includes a zone mask identifying the zones of which each said device is a member.
- 15 3. The method of claim 2 wherein said zone mask comprises:
 - a read mask which, if enabled for a specific device in a particular zone, grants read-only access for said specific device within said particular zone; and
 - a write mask which, if enabled for said specific device in said particular zone grants read and write access for said specific device within said particular zone.
- 20 4. The method of claim 1, further including the step of storing said zone configuration database in a memory in at least one network device connected to the computer network.
- 25 5. The method of claim 4, wherein said network device is selected from the group consisting of: a router, a bridge, a hub, a switch, and a network master.
6. The method of claim 4 wherein said memory is non-volatile.

7. The method of claim 1, further including the step of using a software program running on a device connected to the computer network to create and manage said zone configuration database.
- 5 8. The method of claim 1, wherein said zone configuration database includes a zone mask associated with each logical unit number in a device.
9. The method of claim 1 wherein zone access is controlled by selected network devices through redundant paths in a redundancy group.
- 10 10. The method of claim 1 further including the step of, during an initialization phase, storing, in a memory, unique device ID information for each device.

15

11. A system for zoning devices in a computer network, comprising a zone configuration database which lists each device connected to the computer network, and which allows zone access between devices if and only if they are members of the same zone.
- 20 12. The system of claim 11, wherein said zone configuration database includes a zone mask identifying zones of which each device is a member.
- 25 13. The system of claim 12 wherein said zone mask comprises:
a read mask which, if enabled for a specific device in a particular zone, grants read-only access for said specific device within said particular zone; and
a write mask which, if enabled for said specific device in said particular zone grants read and write access for said specific device within said particular zone.
- 30

14. The system of claim 11 wherein said zone configuration database is stored in a memory in at least one network device connected to the computer network.

5

15. The system of claim 14, wherein said network device is selected from the group consisting of: a router, a bridge, a hub, a switch, and a network master.

10 16. The system of claim 14 wherein said memory is non-volatile.

17. The system of claim 11, wherein said zone configuration database is created and managed by a software program running on a device connected to the computer network.

15

18. The system of claim 11, wherein said zone configuration database includes a zone mask associated with each logical unit number in a device.

20 19. The system of claim 11 wherein zone access is controlled by selected network devices through redundant paths in a redundancy group.

25

20. A system for zoning devices connected to a computer network, comprising:

zoning means which identify zones of which each device is a member, and which allows zone access between devices if and only if they are members of the same zone.

30 21. The system of claim 20, wherein said zoning means includes masking means identifying at least one zone of which each device is a member.

22. The system of claim 21, wherein said masking means comprises:
a read mask which, if enabled for a specific device in a particular
zone, grants read-only access for said specific device within said
particular zone; and
5 a write mask which, if enabled for said specific device in said
particular zone grants read and write access for said specific device
within said particular zone.

10 23. The system of claim 20 wherein said zoning means is stored in a
memory in at least one network device connected to the computer
network.

15 24. The system of claim 23, wherein said network device is selected
from the group consisting of: a router, a bridge, a hub, a switch,
and a network master.

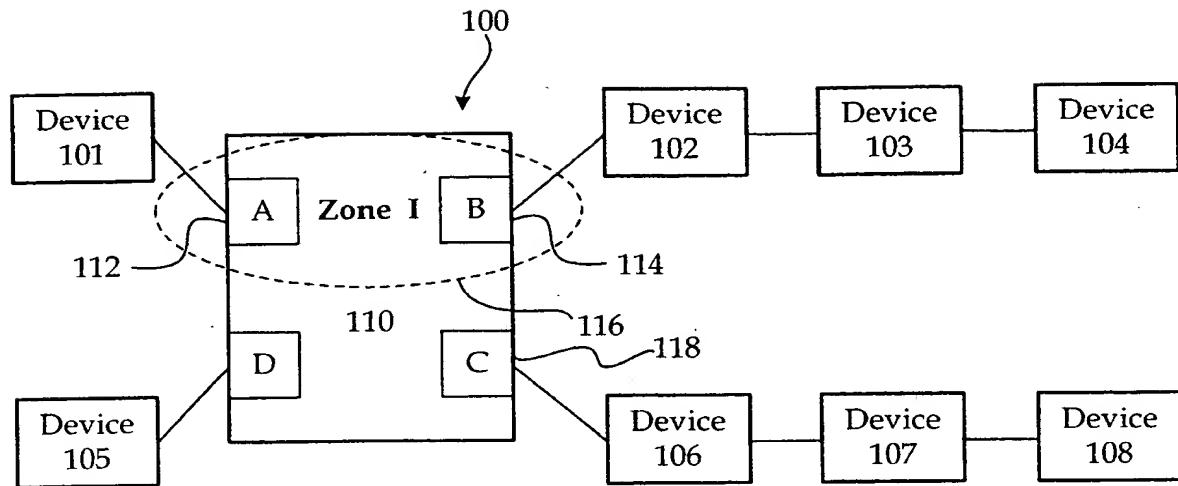
25. The system of claim 23 wherein said memory is non-volatile.

20 26. The system of claim 20 wherein said zoning means is created and
managed by a software program running on a device connected to
the computer network.

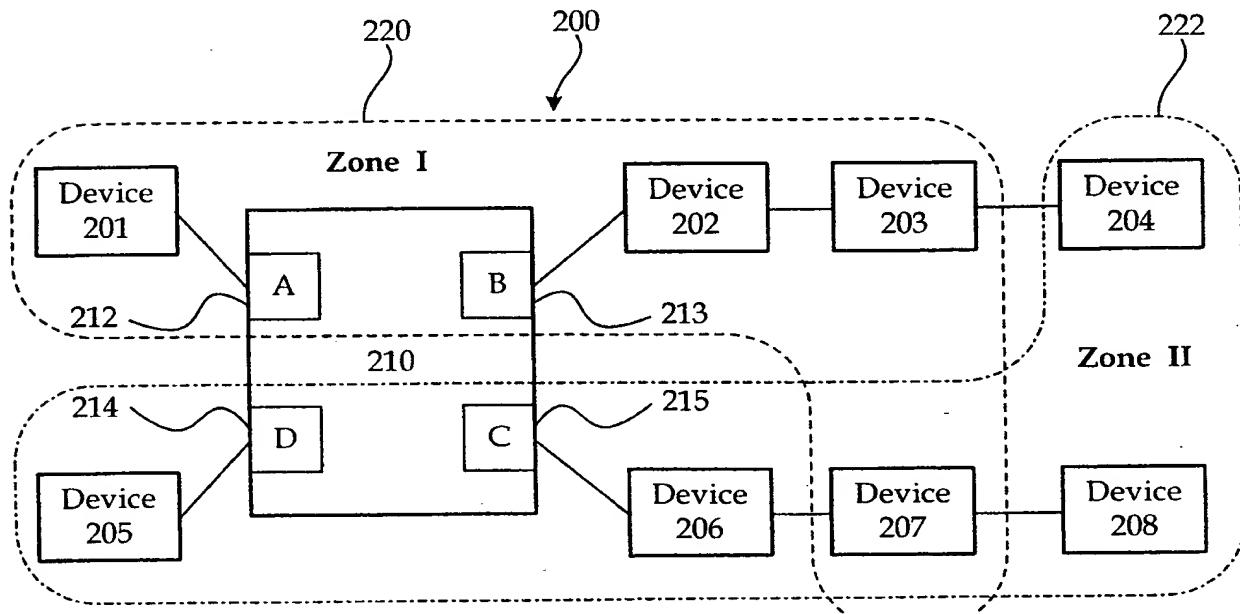
25 27. The system of claim 20, wherein said zoning means includes
masking means associated with each logical unit number in a
device.

30 28. The system of claim 20 wherein zone access is controlled by
selected network devices through redundant paths in a redundancy
group.

1/8



PRIOR ART

FIG. 1**FIG. 2**

2/8

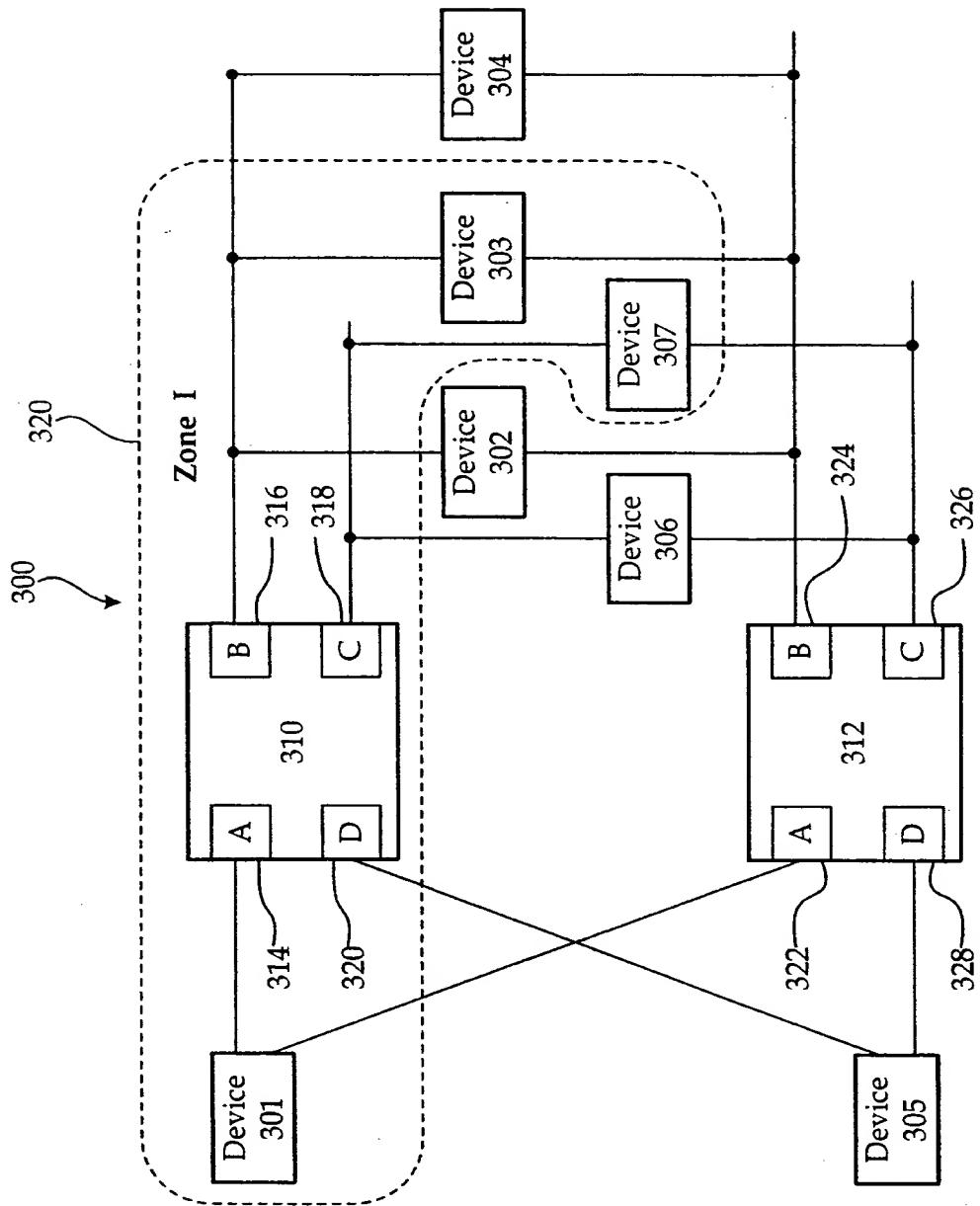
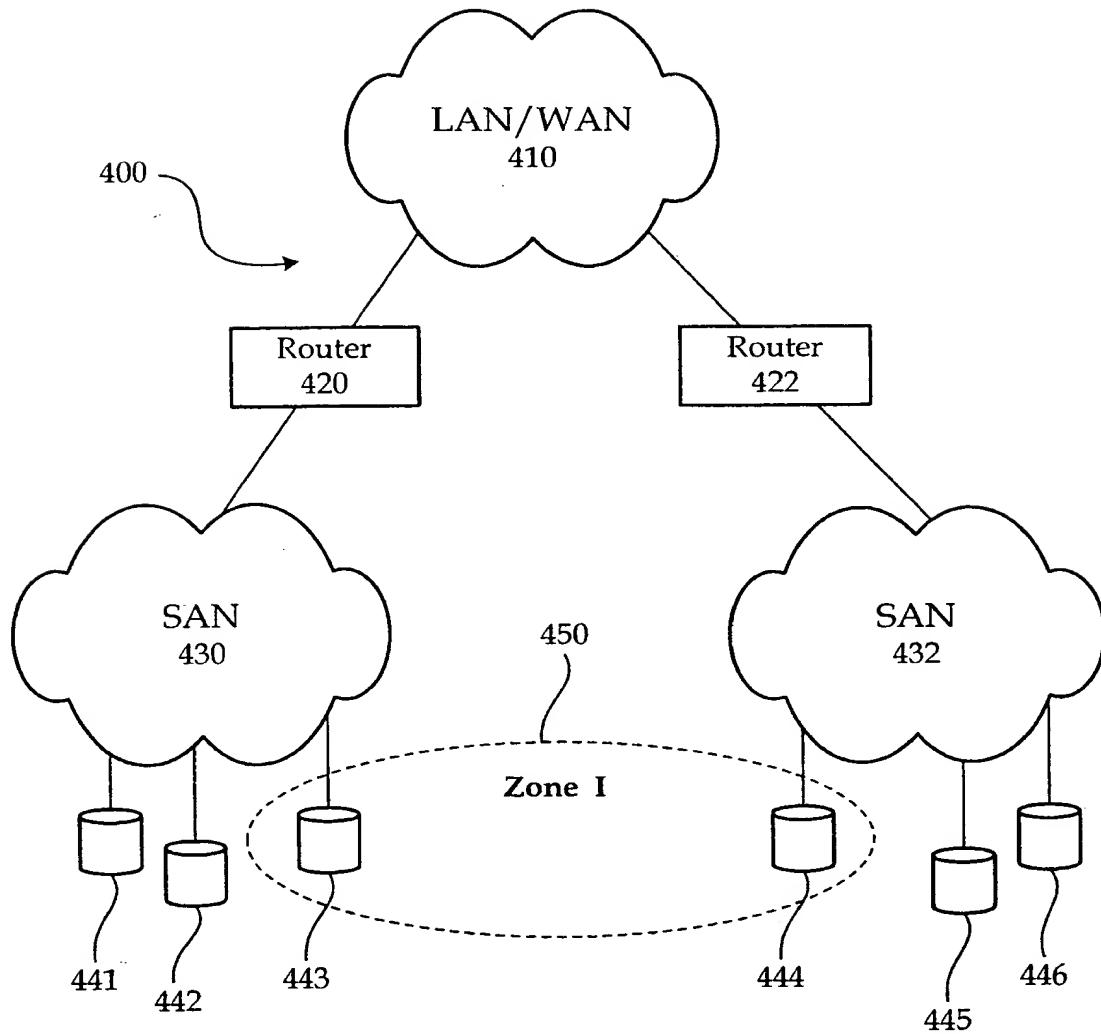
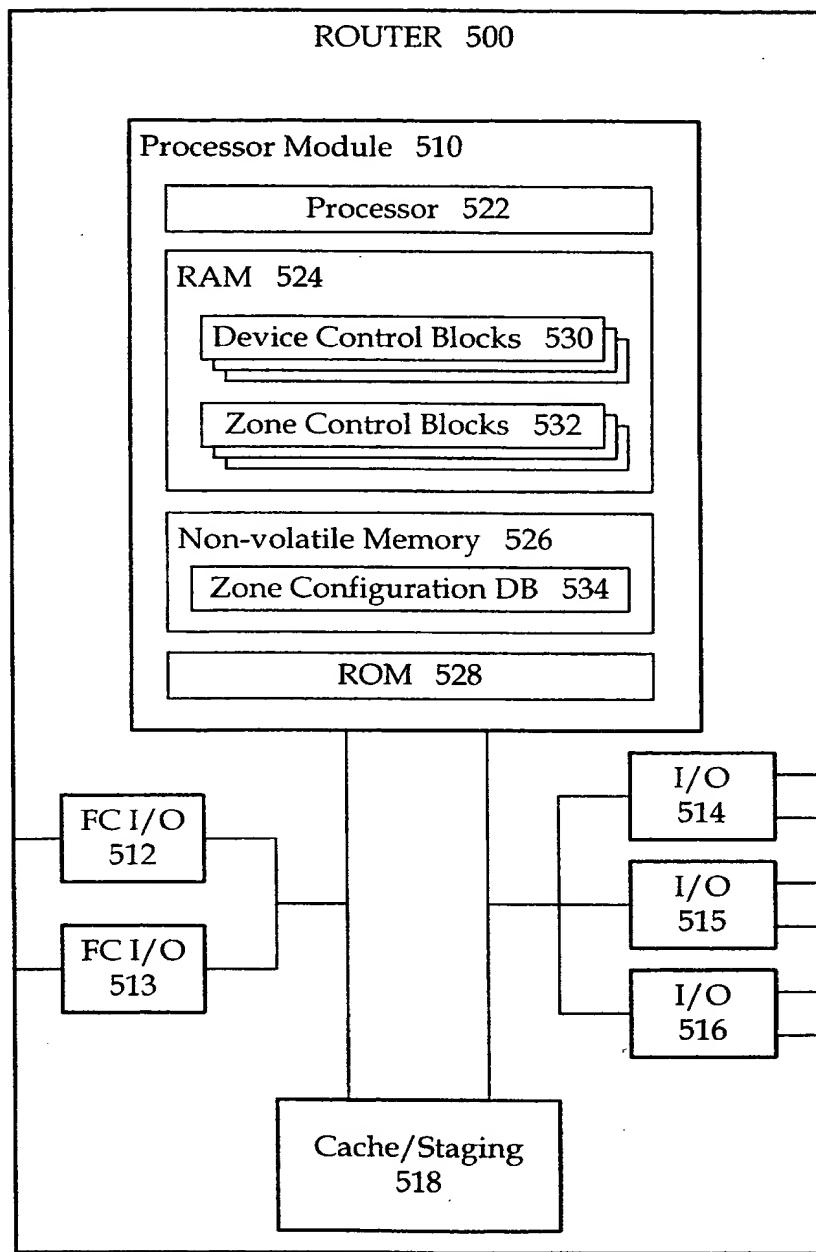


FIG. 3

3/8

**FIG. 4**

**FIG. 5**

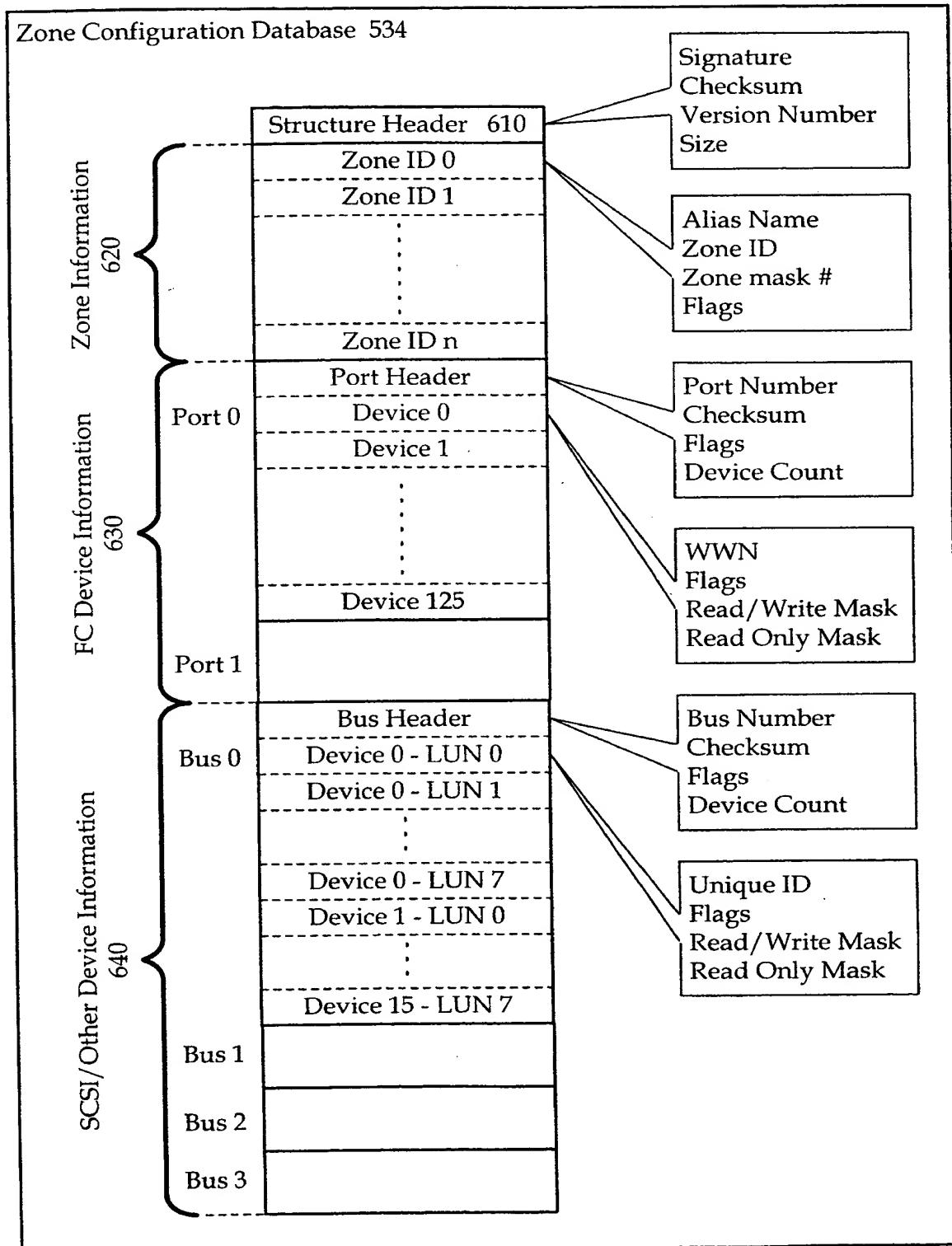
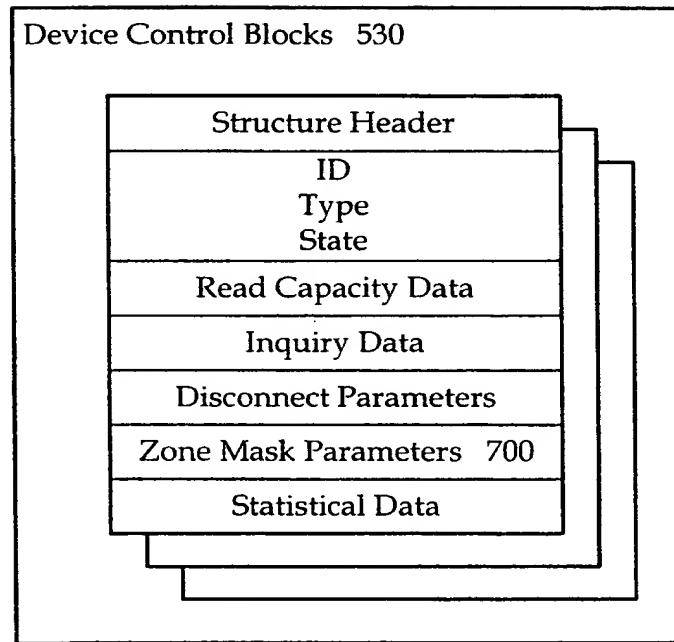


FIG. 6

6/8

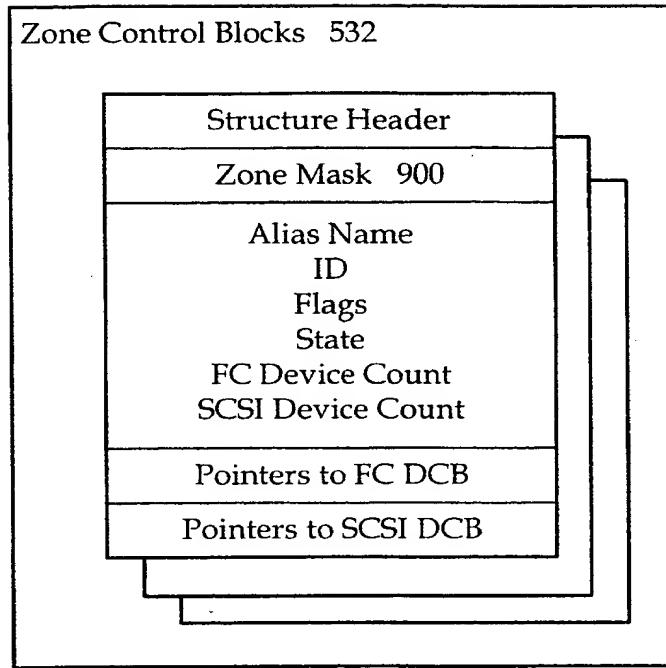
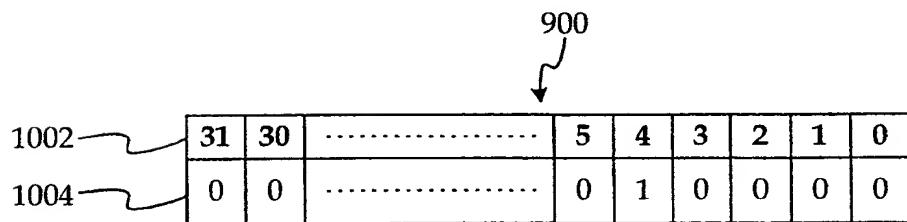
**FIG. 7**

The diagram shows the "Zone Mask Parameters 700" structure as a 10x2 grid of binary values. The columns are labeled 31, 30, ..., 5, 4, 3, 2, 1, 0. The rows are labeled 802, 804, and 806. The values are as follows:

	31	30	...	5	4	3	2	1	0
802	0	0	0	1	0	0	0	1
804	Read Only	0	0	0	1	0	0	1
806	Read/Write	0	0	0	0	1	0	0

FIG. 8

7/8

**FIG. 9****FIG. 10**

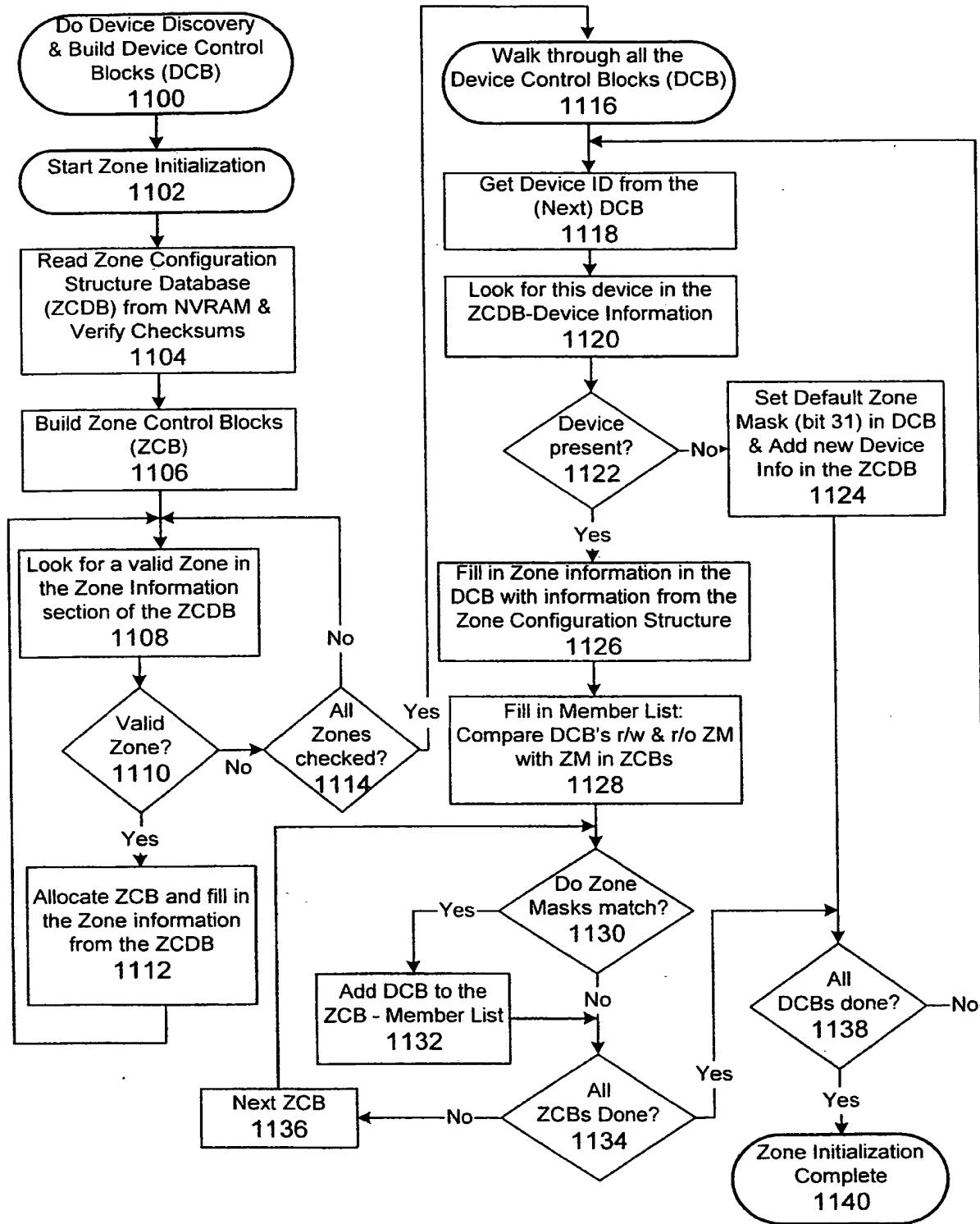


FIG. 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US00/06920

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 15/173, 13/28, 9/00

US CL : 709/225; 710/26; 713/201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/223, 225, 229, 249; 710/26, 200; 713/201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,845,087 A (TREHUS) 01 December 1998, cols. 3-8, especially col. 3 lines 29-36, col. 5 lines 4-19, col. 5 lines 38-55, col. 5 line 66 to col. 6 line 7.	1-2, 4-7, 9-12, 14-17, 19-21, 23-26, 28
X	US 5,515,376 A (MURTHY et al.) 07 May 1996, cols. 1-23, especially col. 7 lines 54-59, col. 13 line 59 to col. 16 line 57.	1-8, 11-18, 20-27
A	US 5,548,649 A (JACOBSON) 20 August 1996, cols. 1-26.	1-28
A	US 5,282,270 (OPPENHEIMER et al.) 25 January 1994, cols. 1-24.	1-28

Further documents are listed in the continuation of Box C. See patent family annex.

- Special categories of cited documents:
- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "A" document defining the general state of the art which is not considered to be of particular relevance
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "L" earlier document published on or after the international filing date
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed
- "E" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 MAY 2000	02 AUG 2000

Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer AHMAD MATAR <i>Joni Hill</i> Telephone No. (703) 305-3800
---	--

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US00/06920

B. FIELDS SEARCHED

Electronic data bases consulted (Name of data base and where practicable terms used):

BRS, ACM Digital Library

search terms: zone, logical unit number, scsi, group, router, bridge, gateway, hub, switch, firewall, SAN, storage area network, fiber channel